REMARKS

The present remarks are in response to the Office Action dated October 20, 2005, in which the Examiner objected to claim 5 as being indefinite, and rejected claims 1-4 and 6-9 and claims 5 and 10 as being unpatentable over the prior art.

In this response, Applicant has amended claim 5 to address and cure the indefiniteness objection. No new matter has been added.

The Applicant responds to the Examiner's Detailed Action and respectfully requests the Examiner place all pending claims detailed in the application in a state of allowance.

A. Indefiniteness Rejection (35 U.S.C. § 112)

The Examiner has rejected claim 5 under 35 U.S.C. §112 as being indefinite. The Applicant has amended claim 5 to clarify and recite "a step of obtaining the signature and at least some of the control operations which are carried out within a single integrated circuit, without any physical access immediately upstream of a module of the integrated circuit, said module adapted to obtain the signature."

B. Prior Art Rejections (35 U.S.C. §§ 102 and 103)

The Examiner has rejected claims 1-4 and 6-9 under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 6,092,191 to Shimbo et al. (hereinafter referred to as "Shimbo"). We submit, however, that Shimbo does not describe or suggest a method or interface carrying the steps at an access interface of a subscriber installation having the steps as recited in Applicant's claims. In fact, Shimbo's security gateway is quite distinct

from the access interface of a subscriber installation as recited in Applicant's claims in several aspects:

a/ The access interface of a subscriber installation, in Applicant's claim, is designed to abide by the contractual framework between a subscriber (e.g., a customer) and a manager of the network (e.g., a provider of services). Therefore, if two customers have signed different contracts, their respective interfaces will differ. In other words, different interfaces correspond to different customers. It follows then, that the signature to be calculated for every respective packet which is about to be transmitted will also be different. In Shimbo, however, the same security gateway is used for different users (see Shimbo, Fig.1). For example, if host H1 in SECTION-A1 NETWORK transmits packets to a host in 104 (organization-C network 104) which is ORGANIZATION-C NET, the security gateway GA will be used, and if H1 transmits packets to another host in 105 (organization-D network 105) which is ORGANIZATION-D NET, the same security gateway GA is used. Therefore, Shimbo describes that only one security gateway is utilized for several hosts and a gateway will be used whenever two hosts, which are in a network path separated by this gateway, are transmitting packets.

b/ Applicant's claims recite the step of carrying out control operations on packets and thereafter, transmitting the packet from the access interface to the concentrating router with each packet transmitted with a signature, authenticating that the packet has been subjected to control operations. This is simply not shown in Shimbo. Rather, Shimbo discloses a packet authentication and encryption/decryption process for security gateways in a network system where packets are being encrypted and appended an authentication code several times, for example, if host H1 in SECTION-A1 NET

transmits packets to a host in 104 which is ORGANIZATION-C NET, according to Shimbo, the packet is appended authentication code in gateways GA11, GA1, GA, and inspected in gateway GA1, GA, GC, respectively. Furthermore, two authentication codes are used, namely, link-by-link codes authenticated and inspected by intermediate nodes and end-by-end codes authenticated and inspected by destination nodes (see Shimbo, col. 11, lines 53-63; col. 11, line 63 – col. 12, line 13). And every security gateway includes both the functions of encryption and authentication (Module 302 of Fig. 3) and the functions of decryption and inspection (Module 303 of Fig. 3; see also Shimbo, col. 12, lines 3-9). However, as recited in Applicant's claim, the access interface of a subscriber in Applicant's invention performs control operations on streams of packets to be transmitted to the concentrating router and only after having carried out those control operations, it transmits packets with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations. Simply put, Shimbo does not describe these steps.

c/ Shimbo discloses that individual security gateways must cooperate with each other in order to, *inter alia*, encrypt the packets. However, not all of the packets will be encrypted (some packets may not be) and thus, errors are notified (see Shimbo, col. 13, lines 6-18). On the other hand, Applicant recites a step of transmitting a packet from the access interface to the concentrating router with each packet transmitted with a signature based on a secret shared with the concentrating router. Therefore, Shimbo does not teach that "each packet" is transmitted with a signature, as recited in Applicant's claim.

d/ In claims 3 and 8, Applicant recites that the code word of the signature is calculated by hashing at least part of a content of the packet, involving the shared secret.

The two methods described in Shimbo set up an authentication key for a set of source host address and destination host address or a set of source host address, destination host address, source port number, and destination port number rather than the content of the packet (see Shimbo, col. 15, lines 29-40 and 49-60). However, in Applicant's claims 3 and 8, the code word of the signature is calculated for "at least part of a content of the packet."

The Examiner also rejected claims 5 and 10 under 35 U.S.C. §103 as being unpatentable over Shimbo in view of U.S. Patent No. 5,726,660 to Purdy et al. (hereinafter referred to as "Purdy") and U.S. Patent No. 4,860,351 to Weingart (hereinafter referred to as "Weingart"). Applicant respectfully disagrees.

As stated in §2143 of the MPEP:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the reference themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references (or references when combined) must teach or suggest all the claim limitations.
>
> The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure. §2143, MPEP Rev. 2.0, May 2004, pg. 2100-129.

As acknowledged by the Examiner, Shimbo does not disclose that the signature and control operations are carried out within a single integrated circuit. Rather, the Examiner cites Purdy as disclosing this feature and concludes that it would have been obvious to one skilled in the art to combine Shimbo and Purdy to arrive at Applicant's claims because "combining multiple functional components on a single integrated circuit reduces manufacturing costs significantly" and one of skill would have been motivated to

perform such modifications to reduce costs (see office action of 10/20/05, page 5). Further, Shimbo is also acknowledged as failing to disclose that there is no physical access immediately upstream of a module of the integrated circuit, the module adapted to obtain the signature. However, Weingart is cited as disclosing this missing feature in the form of an electronic circuit in a tamper resistant package and one of skill would have been motivated to protect the information stored in the circuit.

Applicant submits that dependent claims 5 and 10 each include, by way of their dependencies, *inter alia*, the limitation that a method or an access interface comprise "carrying out, at the access interface, control operations on streams of packets transmitted to the concentrating router," and "transmitting said packet from the access interface to the concentrating router, each packet being transmitted with a signature based on a secret shared with the concentrating router, authenticating that the packet has been subjected to the control operations." As stated above, to establish a *prima facie* obviousness rejection, the Examiner's cited art must teach or suggest all claim limitations.

However, Shimbo, either alone or in combination with Purdy or Weingart, does not describe or suggest a step of obtaining the signature and at least some of the control operations which are carried out within a single integrated circuit, without any physical access immediately upstream of a module of the integrated circuit adapted to obtain the signature. Simply put, there is no such teaching or suggestion in any of these references.

Therefore, Shimbo fails to teach the aforementioned features recited in Applicant's claims.

However, even if we were to assume, *arguendo*, that Shimbo taught such features as noted by the Examiner, which Applicant denies, neither Purdy nor Weingart can be combined with Shimbo.

The reason for the arrangement in Purdy is based on eliminating both the number of individual components and the cost of manufacturing (see Purdy, col. 3, line 66 – col. 4, line 2). However, Purdy is wholly silent on whether the arrangement can provide any security for the system. Shimbo, however, is directed to addressing transmission security rather than eliminating component numbers or manufacturing costs.

In Weingart, the information being protected is stored in a circuit (see Weingart, col. 3, lines 6-11), which means the information is static from the standpoint of the circuit. However, in Shimbo, the information is dynamic, not static. Clearly, the technique of protecting dynamic/transmitting information is completely dissimilar to what is required to protect static/stored information. Therefore, there is no reason why one, provided with Shimbo's static information would ever be motivated to apply the teachings of Weingart as it relates to static/stored information.

Therefore, Applicant submits that none of the above three references, alone or in combination, suggest or describe a method or an access interface with the step of carrying out control operations on packets and thereafter, transmitting the packet from the access interface to the concentrating router with each packet transmitted with a signature, authenticating that the packet has been subjected to control operations, as now recited in claims 1-10.

Consequently, the limitations of claims 1 and 6 are not taught or suggested by the prior art cited. Since the independent claims 1 and 6 overcome the 35 USC § 102

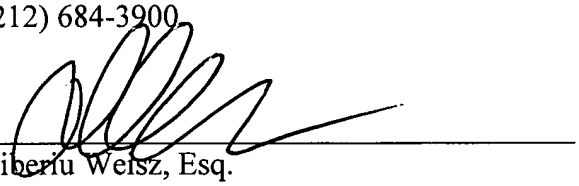
rejection, Applicant submits that their dependent claims 2-5 and 7-10 respectively, also overcome the prior art rejections, are now patentably distinct and in condition for allowance, which action is respectfully requested.

C. Conclusion

For all the foregoing reasons, allowance of all pending claims is respectfully requested.

Respectfully submitted,

GOTTLIEB, RACKMAN & REISMAN, P.C.
Attorneys for Applicant(s)
270 Madison Avenue, 8th Floor
New York, New York 10016
(212) 684-3900



Tiberiu Weisz, Esq.

Dated: January 24, 2006